EXTENDED ABSTRACT: OPTIMAL BLOCK TIME FOR PROOF OF WORK BLOCKCHAINS

This work has been presented at Workshop on Blockchain Horizons, ECIS, Portsmouth, UK June 25th 2018

Sai, Ashish Rajendra, Lero, University of Limerick, Limerick, Ireland, ashish.sai@lero.ie
Buckley, Jim, University of Limerick, Limerick, Ireland, jim.buckley@ul.ie
Le Gear, Andrew, Horizon Globex Ltd., Limerick, Ireland, andrew.legear@horizon-globex.ie

Context

Proof Of Work (PoW) Blockchains such as Bitcoin and Ethereum exhibit a low Transaction Per Second rate (TPS), when compared to centralised transaction processing systems, and that impacts the scalability of the Blockchain. Improving the throughput of Blockchain has long been a fundamental challenge for most PoW Blockchains. Raising block-size in order to increase throughput has been extensively discussed in the Bitcoin community but an agreement on ideal block-size has yet not been achieved due to the security and network implication of a large block in the network (Garzik, Harding, and Johannsson, 2015)(Gervais et al., 2016). Another less discussed procedure is manipulating the block creation time to gain a higher throughput. A faster block creation rate results in a higher Stale Block rate and that has a direct impact on the security of Blockchain. We intend on using a novel PoW Classification model that assesses the acceptance and correctness of transactions under a varying level of difficulty, to classify an instance of blockchain with a threshold Block-time, on the basis of it's resilience to selfish mining and double-spending attacks. This modelling can guide the community towards a more optimal block creation time that can help PoW Blockchains scale without trading off security. The classification model can further be extended to find an optimal block-size.

Objective

Our research intends to quantitatively analyse the impact of mutable block creation time on the security of Blockchains, under a varying level-of-difficulty of mining. On preliminary review of the literature, it can be inferred that research on increasing the throughput has widely been concentrated on manipulation of block-size while lesser research has been conducted on the security implications of block creation time. We propose the use of a novel PoW classifier to find a more optimal block creation time by iterating through the classifier with a variable threshold (block-creation time). In order to evaluate the security, we leverage the existing security evaluation models to simulate the Selfish Mining (Sapirshtein, Sompolinsky, and Zohar, 2017) and the Double Spending attack (Gervais et al., 2016) occurrences on the Blockchain under this changeable block-time. We posit that by using our proposed PoW Classifier, it will be feasible to determine a more optimal block creation time for a given instance of a PoW chain, in terms of its defence against security concerns.

Approach

In machine learning and statistics, classification is described as a mapping of instances to classes based on classification rules defined in the classification model (Michie et al., 1994). We devise a binary classification model with well-defined classes and classification rules. We define the formal context of our model as $< B, C, R >$ where $B = \{B_1, B_2, B_3, ..B_n\}$ is a finite set of n blocks, $C = \{P, N\}$ is a finite set of classes that represent two types of unique blocks in a blockchain. A block with all valid transactions is considered a member of the Positive block class which is denoted by P. A block denoted by N is considered a member of the Negative block class if it contains one or more fraudulent transactions. R is a relation between an instance of B and C e.g. $R(B_1, P) = 1$ signifies that block B_1 is a member of class P. We further consider two hypothesis for hypothesis testing under a block creation time B_t. The Null Hypothesis (H_o) is considered true on acceptance of a block of any class to the largest chain in the network while the alternative hypothesis (H_a) is true if the null hypothesis is false (the block is rejected). We construct a confusion matrix to illustrate the use of classification rules and to evaluate the performance of our model i.e. evaluation of the Blockchain under B_t.

	P	N
H_0	*True Accept*	*False Accept*
H_a	*False Reject*	*True Reject*

The definition of classification rules for our model is as follows, a True Accept is defined by $R(B,P) = 1$, a False accept is defined as $R(B,N) = 0$, a True Reject is defined as $R(B,N) = 1$ and a False Reject is defined as $R(B,P) = 0$. By using our classification model with a sample set containing block members of both classes we can determine True Accept Rate (*TAR*), False Accept Rate (*FAR*), False Reject Rate (*FRR*) and True Reject Rate (*TRR*). Of these, w.r.t. the security concerns, *FRR* and *FAR* are of significant value. On further investigation, we see that *FRR* is the rate of Stale blocks in the network which has a direct implication on the security of the network as established by (Gervais et al .. 2016). *FAR* is the ratio of the number of false accepts to the number of negative blocks and thus a low *FAR* signifies resilience of the Blockchain to attacks. In order to calculate *FAR*, we intend to use a novel approach that takes the difficulty of mining into consideration.

Illustration

We have developed a simulator in order to illustrate the impact of block creation time on the total throughput of the blockchain. Results from this initial simulation suggest that a higher throughput can be achieved using a lower block-time without increasing the block-size. For realistic simulation, we take the average number of transactions per block over a period of 60 days (Feb-02-2018 to Apr-02-2018) of the bitcoin network. It can be seen from the results that a block creation time of **600** seconds yields a **2.06** TPS whereas a block creation time of **60** seconds results in a **20.65** TPS which is a significant improvement. The impact of a new block-creation time on *FAR*/*FRR* can be used to compare the security of the blockchain. We expect to see an increase in *FAR*/*FRR* on decreasing the block-creation time from 600 seconds to 60 seconds. We would like to use our initial findings and extend our simulator to approximate *FAR*/*FRR* to see the effect of varying creation time.

Conclusion

The proposed classifier can be used to quantitatively compare resilience of a blockchain against the Selfish Mining and the Double Spending attacks under a variable block creation time. We intend on extending the model to calculate *FAR* by considering factors such as the difficulty of mining, hashing power and connectivity of the attacker depending upon the timing threshold.
Finally, we have proposed a novel classification model (which needs further enhancement) for PoW blockchains that can be used with efficient simulation to derive a more optimal block-creation time. We also see a potential in using the model for determining ideal block-size by changing the by changing the focus from varying block-creation time to varying block-size.

References

Garzik, J., T. Harding, and D. V. Johannsson (2015). *BIP 100*. URL: https://github.com/jgarzik/bip100/blob/master/bip-0100.mediawiki.

Gervais, A., G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun (2016). "On the Security and Performance of Proof of Work Blockchains." In: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. CCS '16. Vienna, Austria: ACM, pp. 3–16. ISBN: 978-1-4503-4139-4. DOI: 10.1145/2976749.2978341. URL: http://doi.acm.org/10.1145/2976749.2978341.

Michie, D., D. J. Spiegelhalter, C. C. Taylor, and J. Campbell, eds. (1994). *Machine Learning, Neural and Statistical Classification*. Upper Saddle River, NJ, USA: Ellis Horwood. ISBN: 0-13-106360-X.

Sapirshtein, A., Y. Sompolinsky, and A. Zohar (2017). "Optimal Selfish Mining Strategies in Bitcoin." In: *Financial Cryptography and Data Security*. Ed. by J. Grossklags and B. Preneel. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 515–532. ISBN: 978-3-662-54970-4.